State of Iowa - Return on Investment Program / IT Project Evaluation

SECTION 1: PROPOSAL

Tracking Number (For Project Office Use)

Project Name: Information System Security Program

Date: 17 Jul 2000

Agency Point of Contact for Project: Kip Peters

Agency Point of Contact Phone Number / E-mail: 1-5421; Kip.Peters@its.state.ia.us

Executive Sponsor (Agency Director or Designee) Signature: Richard Varn

Is this project necessary for compliance with a Federal standard, initiative, or statute? (If "Yes," cite specific requirement, attach copy of requirement, and explain in Proposal Summary)	❑ Yes	X No
Is this project required by State statute? (If "Yes," explain in Proposal Summary)	X Yes	❑ No
Does this project meet a health, safety or security requirement? (If "Yes," explain in Proposal Summary)	X Yes	❑ No
Is this project necessary for compliance with an enterprise technology standard? (If "Yes," explain in Proposal Summary)	X Yes	❑ No
Does this project contribute to meeting a strategic goal of government? (If "Yes," explain in Proposal Summary)	X Yes	❑ No
Is this a "research and development" project? (If "Yes," explain in Proposal Summary)	❑ Yes	X No

PROPOSAL SUMMARY:

In written detail, explain why the project is being undertaken and the results that are expected. This includes, but is not limited to, the following:

1. A pre-project (before implementation) and a post-project (after implementation) description of the system or process that will be impacted.

   The State of Iowa, in meeting its responsibilities to supply effective State services, plans to provide greater access and new services to State agencies, citizens, and business partners using new and existing State information systems. Sharing and making information available at the enterprise level presents both opportunities and challenges. The State of Iowa has the opportunity to become a leader in providing access to State information at the inter-agency and public levels. The challenge is to ensure that communications, information technology, tools, systems, and personnel provide a non-intrusive security environment while maintaining confidentiality, integrity, availability, and accountability of the information and information

resources. This environment must provide reliable and secure information, in any required form, where and when needed.

In today's State of Iowa Enterprise, many systems are interconnected in some way. Because of this, security vulnerabilities in one system have an adverse effect on the security posture of other interfacing systems. Therefore, enterprise security is defined by the aggregate security posture of the State systems comprising the enterprise. The problem is, while many State agencies have a high degree of technical capability in controlling and protecting their information technology assets, this level of competence is not consistent throughout the enterprise, contributing to an unpredictable enterprise security posture.

The Information System Security Program (ISSP) is designed to do several things. It will increase the level of consistency in agency security programs by developing and helping the agencies to conform to enterprise security policies, standards, and guidelines. It will also develop and implement a user security awareness training program, conduct network vulnerability assessments, establish and operate a risk management program, assist agencies with ad hoc security projects, plan, develop, and implement a State of Iowa Public Key Infrastructure (PKI), facilitate communication among the agencies concerning security vulnerabilities, incidents, and knowledge, develop security-related checklists and procedures, and identify, plan for, fund, and implement enterprise-level security technologies.

Regarding public key infrastructure, PKI is a technology which has emerged due to the need for enhanced security, integrity, and non-repudiation of electronic transactions. The State of Iowa, following the guidelines contained in the Uniform Electronic Transactions Act (UETA), passed UETA for Iowa which assesses that where a transaction requires a signature, a digital signature will satisfy the requirement. Although the law does not mention PKI explicitly, PKI is widely becoming accepted as the standard for digital signatures.

The State has asserted in House File 2205 that all transactions with the State will be available electronically by July 2003. PKI will enable Iowa to realize the intent of PKI by allowing citizens, businesses, and governments to perform transactions electronically with each other.

PKI will allow a variety of entities to perform transactions electronically with the state. Possible affected transactions are:

Affected Transaction Area	Implementations
Government to Government	Timesheets Purchasing Encrypted Emails Accounting Processes
Government to Business	Permits, Licenses and Permission Corporate Filings Tax Filings Procurements Other Online Transactions
Government to Citizen	Professional Licensing Recreational Licenses Tax Filings Drivers Licenses Requests for Birth, Marriage, and Death Certificates Other Online Transactions

Baltimore Technologies was recently contracted with the State to assist in identifying PKI needs and requirements. The following documents are available for review:

- Requirements Document
- Suggested Architecture
- Cost Analysis
- Vendor Analysis

Baltimore, through interviews with State agencies, identified major areas for PKI projects. The ITD feels that an internal State implementation of PKI will help to educate employees and set the stage for additional PKI projects. Therefore, in this initial permeation of digital signatures, the ITD will establish a relationship with a PKI vendor to act as a Certificate Authority for the State of Iowa, and then establish digital signatures for State Employees and enable secure e-mail as a pilot project. At this point, the ITD will work with the agencies to identify further PKI projects and develop a PKI roadmap.

2. A summary of the extent to which the project provides tangible and intangible benefits to either Iowa citizens or to State government. Included would be such items as qualifying for additional matching funds, improving the quality of life, reducing the government hassle factor, providing enhanced services, improving work processes, complying with enterprise technology standards, meeting a strategic goal, avoiding the loss of matching funds, avoiding program penalties/sanctions or interest charges, avoiding risks to health/security/safety, complying with federal or state laws, etc.

   The result of these security and PKI initiatives will be an enterprise with enhanced security and appropriate access to all the systems that make up the enterprise, thereby benefiting the agencies, their partners, and their customers. Important information will be available to authorized users while also being protected from disclosure and unauthorized change. This is important not only to State government, but also to its citizens and business partners.

3. A summary that identifies the project stakeholders and how they are impacted by the project.

   A program of this magnitude has many stakeholders; it is not unreasonable to identify all State citizens, agencies, and business partners as stakeholders that will be impacted by the project. All present Iowa citizens, and many past citizens, have personal information that is stored, processed, and/or disseminated by State government computer systems. They all have a stake in the protection of that information. All agencies, even non-participating agencies, will benefit by the increased security of the enterprise, since most of these agencies either share some of the same architecture or have information that is stored on Iowa mainframes or other agency systems. In today's interconnected world, if a vulnerability leads to a compromise in one system, it may lead to unintended privileged access to information on other systems. If business partners are to conduct business electronically with the State, it is important that their interests are protected as well.

The following paragraphs address the answers to the six questions above:

1. *Federal standard, initiative, or statute:* While the Information Systems Security Program itself is not necessary for compliance with any known federal standards, initiatives, or statutes, the program has assisted agencies and the State in meeting federal security requirements, directives, and guidelines, and will continue to do so in the future. In particular, the program has previously assisted the Department of Revenue and Finance (both with the department itself and the Enterprise Data Warehouse), Department of Human Services, and Information Technology Department with Internal Revenue Service (IRS) security audits while clarifying and helping

these departments meet IRS security requirements. Also, the program continues to assist the Department of Public Safety (DPS) meet requirements dictated by the Criminal Justice Information System Security Policy, published by the Federal Bureau of Investigation.

2. *State statute:* House File 2205 (signed into law on May 15, 2000) stipulates that most Executive Branch agencies, departments, boards, commissions, authorities, and institutions must "send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and signatures" by July 1, 2003, unless a waiver from the Department of Management is obtained. The Security Program will include a public key infrastructure which will be instrumental in making this a reality.
3. *Security requirement:* Not only does the program help meet security requirements, it will be generating security requirements for the State of Iowa Enterprise. The program also contributes to the safety of State citizens by working with DPS in securing their networks and information. Although DPS is not one of the participating agencies as defined by Senate File 2395, it has been and will continue to participate in the ISSP.
4. *Enterprise technology standard:* The program will be establishing enterprise technology standards; specifically, standards that deal with security of information and information systems.
5. *Strategic goal of government:* The program is essential in meeting the State of Iowa's Digital Government and E-Commerce goals. Without effective security controls and practices in place, the goal of "If you have to wait in line it should be on-line" will ultimately fail. In the absence of an enterprise program, individual programs will implement security independently and at differing levels of assurance; an enterprise program provides a cohesive security umbrella, ensuring that security efforts meet a consistent security policy, are adequate, and are cost-effective. Likewise, a single State of Iowa PKI will be essential in meeting these goals by making the promises of digital signatures and true authentication reality. A PKI will enable users, including State employees, agencies, business partners, and citizens, to conduct business with the State in an effective, safe, and secure manner. Critical information will be available to authorized users when needed, and it will be protected from disclosure and unauthorized change. State agencies have many electronic plans and goals, including secure e-mail, secure web browser and server connections, virtual private networks, form signing, file encryption, and wireless applications; a State of Iowa PKI will be a key enabler of achieving these goals.
6. *Research and development:* This is not a research and development (R&D) project; however, some R&D will be conducted by necessity during its performance.

SECTION 2: PROJECT PLAN

Individual project plans will vary depending upon the size and complexity of the project. A project plan includes the following information:

1. Agency Information

Project Executive Sponsor Responsibilities: Identify, in Section I, the executive who is the sponsor of the project. The sponsor must have the authority to ensure that adequate resources are available for the entire project, that there is commitment and support for the project, and that the organization will achieve successful project implementation.

The Chief Information Officer (CIO) is the sponsor of the project. With adequate funding, the CIO will ensure that adequate resources are made available for the project. Unwavering support for the project has been committed by both the CIO and the Information Technology Department (ITD). Part of the CIO's responsibilities are to promote the project to the Governor and the Legislature, while solving any disputes that may arise that the Chief Information Security Officer (CISO) will be unable to resolve.

Organization Skills: Identify the skills that are necessary for successful project implementation. Identify which of these skills are available within the agency and the source(s) and acquisition plan for the skills that are lacking.

The skills necessary for successful project implementation include the following:

- Project management
- Technical security issues, controls, hardware, and software
- Security policies, procedures, and other documentation
- Security-related standards and best practices
- Security training and awareness
- Security threats and vulnerabilities
- Security patches, fixes, and other countermeasures
- Viruses and other malicious logic
- Vulnerability assessments
- Risk management
- Physical security
- Operations security
- Public key infrastructure (PKI) planning and implementation
- PKI policy
- PKI management
- PKI operations
- PKI application development
- Marketing (for PKI applications)

The project management and non-PKI skills exist for the most part in the agency; however, they reside in an extremely limited number of people and in differing levels of expertise. Moreover, only one person in the agency is dedicated to the security program, and part of his responsibilities include the security of ITD and PKI. Only two individuals are responsible for the PKI portion; both are relatively knowledgeable of PKI, but neither one has been involved in a PKI implementation, and neither one is dedicated

full-time to PKI. For this program to succeed, additional personnel are necessary. At this time, it has been indicated that contractors will have to be used to supplement existing agency expertise. Part of the funding currently being requested will be used to hire competent contractors to assist with the security and PKI implementations. Over time, it is anticipated that FTEs will be made available and full-time State security employees will be hired when possible.

2. Project Information

Mission, Goals, Objectives: The project plan should clearly demonstrate that the project has developed from an idea to a detailed plan of action. The project plan must link the project to an agency's mission, goals, and objectives and define project objectives and how they will be reached.

The ultimate goal of the ISSP is to ensure the availability, integrity, and confidentiality of enterprise information and information technology resources by implementing a statewide enterprise security program that is uniformly implemented and consistently enforced throughout each State entity (agency, commission, authority, etc.). ITD has also been identified as the entity to integrate and standardize E-Commerce functions across the enterprise. A State of Iowa PKI will enable E-Commerce in the State of Iowa providing for enhanced access to government services as directed in House File 2205. Other goals include:

- Identifying opportunities for agencies to collaborate on security technology purchases, maintenance, and training, saving money through economies of scale while increasing security.
- Protecting the State of Iowa from liabilities and embarrassment associated with the loss/damage/exposure of sensitive and confidential data.
- Promoting the exchange of information among State of Iowa organizations to facilitate the development of knowledge and understanding regarding information security.
- Establish a relationship with a PKI vendor as a certificate authority and solutions provider.

Program objectives are to:

- Develop, implement, and monitor the ISSP.
- Educate and train users in security awareness.
- Integrate security into each system life cycle.
- Explore and apply technology.
- Assess the security posture of the enterprise and agency systems.
- Ensure security controls are designed into enterprise and agency systems.
- Detect external and internal attacks, as well as internal misuse of systems.
- Provide a method for State agencies to provide digital signatures to staff.
- Provide a method for securing e-mail across the enterprise.

These goals and objectives contribute to the ITD's mission of providing quality information services and technology standards for State agencies.

A. **Expectations**: A description of the purpose or reason that the effort is being undertaken and the results that are anticipated.

The State of Iowa, in meeting its responsibilities to supply effective State services, plans to provide greater access and new services to State agencies, citizens, and business partners using new and existing State information systems. Sharing and making information available at the enterprise level presents both opportunities and challenges. The State of Iowa has the opportunity to become a leader in providing access to State information at the inter-agency and public levels. The challenge is to ensure that communications, information technology, tools, systems, and personnel provide a non-intrusive security environment while maintaining confidentiality, integrity, availability, and accountability of the information and information resources. This environment must provide reliable and secure information, in any required form, where and when needed.

In today's State of Iowa Enterprise, many systems are interconnected in some way. Because of this, security vulnerabilities in one system have an adverse effect on the security posture of other interfacing systems. Therefore, enterprise security is defined by the aggregate security posture of the State systems comprising the enterprise. The problem is, while many State agencies have a high degree of technical capability in controlling and protecting their information technology assets, this level of competence is not consistent throughout the enterprise, contributing to an unpredictable enterprise security posture.

The Information System Security Program (ISSP) is designed to do several things. It will increase the level of consistency in agency security programs by developing and helping the agencies to conform to enterprise security policies, standards, and guidelines. It will also develop and implement a user security awareness training program, conduct network vulnerability assessments, establish and operate a risk management program, assist agencies with ad hoc security projects, plan, develop, and implement a State of Iowa Public Key Infrastructure (PKI), facilitate communication among the agencies concerning security vulnerabilities, incidents, and knowledge, develop security-related checklists and procedures, as well as identify, plan for, fund, and implement enterprise-level security technologies.

The result will be an enterprise with enhanced security and appropriate access to all the systems that make up the enterprise, thereby benefiting the agencies, their partners, and their customers. Important information will be available to authorized users, while also being protected from disclosure and unauthorized change. This is important not only to State government, but also to its citizens and business partners.

B. **Measures**: A description of the set of beliefs, tradeoffs and philosophies that govern the results of the project and their attainment. How is the project to be judged or valued? What criteria will be used to determine if the project is successful? What happens if the project fails?

It is difficult to ascertain the successful nature of a security program. Most security programs are deemed successful if nothing happens; that is, no major incident occurs, or a minimum number of incidents occur and are recovered from in a timely and cost effective manner. However, that is not a truly accurate assessment, as a company, state government, or other entity can escape incident just by being lucky.

The State of Iowa ISSP can be determined successful if the following items become reality:

- Security problems are identified, prioritized, and fixed.
- Users are educated on security issues and awareness.
- Consistent security policies are developed, implemented, and enforced (at both the enterprise and agency levels).
- Security is considered throughout the system life cycle.
- Security standards are developed and promulgated.
- Communication among State security professionals is enhanced.
- A State of Iowa root certificate authority is configured and put into operation.
- Agency e-mail users are able to send secure e-mail by utilizing the results of the initial phase of the State of Iowa PKI.
- E-Commerce is enabled with a standard approach.

If the project fails, then the situation remains what it is today; at best, multiple ad-hoc security programs implementing security with differing levels of assurance.

C. **Environment:** Who will provide input (e.g., businesses, other agencies, citizens) into the development of the solution? Are others creating similar or related projects? Are there cooperation opportunities?

State agencies will be actively involved in the development and implementation of the ISSP and the State of Iowa PKI. The program will depend upon the input and participation of the agencies; they will be developing their own policies, implementing their own procedures, and securing their own systems under the guidance of the ISSP. The ISSP is not intended to actively (i.e., hands-on) secure every agency and every system; it is intended to provide a higher level of guidance, coordination, and communication. All agencies will provide input based upon their current business processes and user interaction.

D. **Project Management and Risk Mitigation**: A description of how you plan to manage the project budget, project scope, vendors, contracts and business process change (if applicable). Describe how you plan to mitigate project risk.

The project will be managed utilizing Microsoft Project software and will be consistent with the ITD project manual. Contractors will be required to provide weekly status reports and bill the State in bi-weekly increments. Changes will be fed through the office of the CISO, and most activities will be coordinated with the Information Technology Management Committee, the Executive Security Committee (to be established by the program), and/or the agencies themselves.

E. **Security / Data Integrity / Data Accuracy / Information Privacy**: A description of the security requirements of the project? How will these requirements be integrated into the project and tested. What measures will be taken to insure data integrity, data accuracy and information privacy?

State of Iowa security vulnerability and risk information is critical information and will be protected as such by a combination of technical and procedural security controls. The final PKI provider will have to provide proof of their internal security of the certificate authority. Individual registration authorities will have to be secured according to the certificate policy and the certification practice statement.

3. Current Technology Environment (Describe the following):

The security portion of this project does not lend itself to readily identify the hardware and software of the current and proposed environment. This is due to three reasons. First, the program is intended to address the entire State of Iowa Enterprise comprised of many interfacing client, server, midrange, and mainframe systems. This includes all systems of all types of hardware and software, many of which are unknown at this time, in many different logical and physical environments, interfacing with both internal and external systems. Second, the program by its very nature has some unknown elements at this point. The risk management program itself must first be developed and implemented in order to determine what security features are lacking; once the deficits are identified the needs will have to be prioritized and implemented as funding permits. Third, the program isn't 100% hardware and software oriented. Much of the security program involves policy, procedures, guidelines, communication, education, and awareness.

The PKI portion will mainly affect e-mail and groupware systems including, but not limited to, Outlook and Notes mail clients running on a variety of Microsoft Windows servers and clients. E-mail will support both encryption and electronic signatures. An interface from License 2000 to the State's accounting system will be present to process money transfers and audit transactions, as well as to CyberCash for the processing of credit card transactions.

A. **Software (Client Side / Server Side / Midrange / Mainframe)**

- Application software
- Operating system software
- Interfaces to other systems: Identify important or major interfaces to internal and external systems

B. **Hardware (Client Side / Server Side / Mid-range / Mainframe):**

- Platform, operating system, storage and physical environmental requirements.
- Connectivity and Bandwidth: If applicable, describe logical and physical connectivity.
- Interfaces to other systems: Identify important or major interfaces to internal and external systems.

4. Proposed Environment (Describe the following):

Please see response to #3.

A. Software (Client Side / Server side / Mid-range / Mainframe)

- Application software.
- Operating system software.
- Interfaces to other systems: Identify important or major interfaces to internal and external systems.
- General parameters if specific parameters are unknown or to be determined.

B. Hardware (Client Side / Server Side / Mid-range / Mainframe)

- Platform, operating system, storage and physical environmental requirements.
- Connectivity and Bandwidth: If applicable, describe logical and physical connectivity.
- Interfaces to other systems: Identify important or major interfaces to internal and external systems.
- General parameters if specific parameters are unknown or to be determined.

Data Elements: If the project creates a new database the project plan should include the specific software involved and a general description of the data elements.

Project Schedule: A schedule that includes: time lines, resources, tasks, checkpoints, deliverables and responsible parties.

For the project schedule, please see the attached Microsoft Project schedule. This schedule is based on the current working schedule which was completed based on the current situation; that is, that personnel resources are limited. The attached schedule anticipates being able to hire three to four full-time contractors. The PKI implementation schedule will be determined upon vendor selection.

SECTION 3: Return On Investment (ROI) Financial Analysis

Project Budget:

Provide the estimated project cost by expense category.

Personnel	$ 127,500.00
Software	$ 137,000.00
Hardware	$ 100,000.00
Training	$ 35,000.00
Facilities	$
Professional Services	$ 762,480.00
Supplies	$ 1,000.00
Other (Specify)	$
Total	$ 1,162,980.00

Project Funding:

Provide the estimated project cost by funding source.

State Funds	$ 1,162,980.00	100	% of total cost
Federal Funds	$		% of total cost
Local Gov. Funds	$		% of total cost
Private Funds	$		% of total cost
Other Funds (Specify)	$		% of total cost
Total Cost:	$		% of total cost

How much of the cost would be incurred by your agency from normal operating budgets (staff, equipment, etc.)? ..... $ 0.00 0 %

How much of the cost would be paid by "requested IT project funding"? .. $ 1,162,980.00 100 %

Provide the estimated project cost by fiscal year: FY 2001 $ 1,162,980.00

FY 2002 $ 0

FY 2003 $ 0

Note: In addition to the funds requested above, there is a need to fund the State security effort beyond FY01. It is estimated that approximately $1,000,000 will be required in each of the next two fiscal years to implement new security projects and initiatives. Annual maintenance costs for the project described in this document are expected to be approximately $175,000.

ROI Financial Worksheet Directions (Attach Written Detail as Requested):

Annual Pre-Project Cost -- Quantify, in written detail, all actual State government direct and indirect costs (personnel, support, equipment, etc.) associated with the activity, system or process prior to project implementation. This section should be completed only if State government costs are expected to be reduced as a result of project implementation.

Annual Post-Project Cost -- Quantify, in written detail, all estimated State government direct and indirect costs associated with activity, system or process after project implementation. This section should be completed only if State government costs are expected to be reduced as a result of project implementation.

State Government Benefit -- Subtract the total "Annual Post-Project Cost" from the total "Annual Pre-Project Cost." This section should be completed only if State government costs are expected to be reduced as a result of project implementation.

Citizen Benefit -- Quantify, in written detail, the estimated annual value of the project to Iowa citizens. This includes the "hard cost" value of avoiding expenses (hidden taxes) related to conducting business with State government. These expenses may be of a personal or business nature. They could be related to transportation, the time expended on or waiting for the manual processing of governmental paperwork such as licenses or applications, taking time off work, mailing, or other similar expenses.

Opportunity Value/Risk or Loss Avoidance Benefit -- Quantify, in written detail, the estimated annual benefit to Iowa citizens or to State government. This could include such items as qualifying for additional matching funds, avoiding the loss of matching funds, avoiding program penalties/sanctions or interest charges, avoiding risks to health/security/safety, avoiding the consequences of not complying with State or federal laws, providing enhanced services, avoiding the consequences of not complying with enterprise technology standards, etc.

Total Annual Project Benefit -- Add the values of all annual benefit categories.

Total Annual Project Cost -- Quantify, in written detail, the estimated annual new cost necessary to implement and maintain the project including consulting fees, equipment retirement, ongoing expenses (i.e. labor, etc.), other technology (hardware, software and development), and any other specifically identifiable project related expense. In general, to calculate the annual hardware cost, divide the hardware and associated costs by three (3), the useful life. In general, to calculate the annual software cost, divide the software and associated costs by four (4), the useful life. This may require assigning consulting fees to hardware cost or to software cost. A different useful life may be used if it can be documented.

Benefit / Cost Ratio – Divide the "Total Annual Project Benefit" by the "Total Annual Project Cost." If the resulting figure is greater than one (1.00), then the annual project benefits exceed the annual project cost. If the resulting figure is less than one (1.00), then the annual project benefits are less than the annual project cost.

ROI -- Subtract the "Total Annual Project Cost" from the "Total Annual Project Benefit" and divide by the amount of the project funds requested.

Benefits Not Cost Related or Quantifiable -- List the project benefits and articulate, in written detail, why they (IT innovation, unique system application, utilization of new technology, hidden taxes, improving the quality of life, reducing the government hassle factor, meeting a strategic goal, etc.) are not cost related or quantifiable. Rate the importance of these benefits on a "1 – 10" basis, with "10" being of highest importance. Check the "Benefits Not Cost Related or Quantifiable" box in the applicable row.

ROI Financial Worksheet

Annual Pre-Project Cost - How You Perform The Function(s) Now	
FTE Cost (salary plus benefits):	
Support Cost (i.e. office supplies, telephone, pagers, travel, etc.):	
Other Cost (expense items other than FTEs & support costs, i.e. indirect costs if applicable, etc.):	
A. Total Annual Pre-Project Cost:	
Annual Post-Project Cost – How You Propose to Perform the Function(s)	
FTE Cost:	
Support Cost (i.e. office supplies, telephone, pagers, travel, etc.):	
Other Cost (expense items other than FTEs & support costs, i.e. indirect costs if applicable, etc.):	
B. Total Annual Post-Project Cost:	
State Government Benefit (= A-B):	
Annual Benefit Summary	
State Government Benefit:	
Citizen Benefit (including quantifiable "hidden taxes"):	
Opportunity Value and Risk/Loss Avoidance Benefit:	
C. Total Annual Project Benefit:	
D. Total Annual Project Cost:	
Benefit / Cost Ratio (C / D):	———
ROI (C – D / Project Funds Requested):	_____%
X Benefits Not Cost Related or Quantifiable (including non-quantifiable "hidden taxes")	

Due to the nature of the project for which funding is being sought, the calculation of a return on investment is not possible. The implementation of the Information Systems Security Program will not necessarily lead to monetary savings. In fact, some costs in some agencies could increase slightly. This could be due to additional monitoring that must take place or additional equipment required to further secure certain IT systems. Other agencies may decrease costs as individual security programs are streamlined, consolidated, and implemented in a more cost-effective manner.

There are significant benefits to be realized by implementing this program. Having consistent, specific security policies (rating = 10) will ensure that all agencies have the appropriate level of oversight on information security. Assessing system security and putting appropriate technical and procedural measures in place (9) to close security gaps will help ensure that intentional and unintentional breaches do not occur. Published averages vary considerably, but one thing is certain: the monetary costs associated with security incidents are substantial. These costs may include those associated with system rebuild, damage assessment, data recovery, system unavailability, civil lawsuit, and data integrity verification.

The non-monetary costs of potential breaches range anywhere from embarrassment (5) to loss of life (10). These costs are significant as well and will be minimized by implementing an enterprise information security solution.

Other benefits include the following items:

- State government will fulfill its statutory requirements with regard to data privacy and data integrity concerns (10).
- This project will raise and maintain awareness of computer security with individual agencies and will provide an enterprise direction for individual agency security programs (8).
- Citizens of Iowa will have an increased confidence in their government's ability to secure confidential data from accidental release (7).
- Money will no longer be wasted on inadequate, inferior, and/or non-standard security solutions (8).
- The State of Iowa will be able to pursue initiatives of providing greater access to information and services to employees and citizens while protecting sensitive information (9).
- The State of Iowa will be better able to obtain its Digital Government and E-Commerce goals (9).
- State citizens, businesses, and employees will have access to information and will be able to conduct business on-line, reducing the frustrations often evident in doing business with the State government bureaucracy (8).

The State of Iowa Public Key Infrastructure and associate E-Commerce and Digital Government initiatives will involve multiple agencies and ROI savings and benefits will be determined on a project by project basis. In order to participate in the system, each agency will be required to complete the ROI Financial Worksheet above. Once those are completed for those agencies, then the State can gauge cost savings over time.